JOURNAL OF NUMBER THEORY 3, 226–239 (1971)

# Remarks on Principal Factors in a Relative Cubic Field*

PIERRE BARRUCAND†

*Institut Blaise Pascal, Paris, France*

AND

HARVEY COHN‡

*Department of Mathematics, University of Arizona, Tucson, Arizona 85721*

*Communicated by H. B. Mann*

Received March 16, 1970

This work supplements an earlier paper in this journal (Vol. 2, 1970, pp. 7–21) on "principal factors" (essentially principal ramified ideals) in the pure cubic $k_3 = Q(n^{1/3})$ over $Q$. The ideas are extended to the Kummer field $k_6 = k_3(\rho)$ over the cyclotomic cubic $k_2 = Q(\rho)$. Here the Hilbert theory brings in the nonexistence of a unit in $k_6$ of relative norm $\rho$. As a typical result, for $n = q$ (prime) $\equiv 2,5 \pmod 9$, the principal factor must exist in $k_6$ and $k_3$, leading to the solvability of the norm equation $x^3 + qy^3 + q^2z^3 - 3qxyz = 3$. Also for $n = q \equiv -1 \pmod 9$, there is a unit of relative norm $\rho$ when the class number of $k_3$ is not $\equiv 0 \pmod 3$.

## 10. RELATIVE PRINCIPAL FACTORIZATION

In the preceding study of cubic class number [15], the concept of principal factorization played a vital role in the purely rational approach. To see the ideas in broader perspective, e.g., as a projection of Hilbert's Theory of Kummer Fields [7] to the rationals, it is important to restate principal factorization in relative fields.

Generally, let $K$ be a field of degree $l$ relative to $k$ and let $\mathfrak{r}_1, \ldots, \mathfrak{r}_t$ be the set of totally (relatively) ramified prime ideals of $k$. Thus $\mathfrak{r}_i$ factors in $K$ as

$$\mathfrak{r}_i = \mathfrak{R}_i^l. \tag{10.1}$$

* This paper continues the earlier work of the authors [15]. The sections and the new bibliographical items are numbered consecutively with it. The symbols from [15] such as $t$, $e$, $h$,..., will now be referred to as $t_3$, $e_3$, $h_3$,....

† Research supported by Centre National de la Récherche Scientifique.

‡ Research supported by National Science Foundation (Grant P-6423).

The relative discriminant $\mathfrak{d}$ of $K$ over $k$, will, of course, have the factors $\mathfrak{r}_i$. (See [7, 19]). Now we consider the multiplicative group $G'$ of fractional ideals $\mathfrak{A}$ generated by $\mathfrak{R}_i$. Call $G$ the subgroup defined by the homomorphism with the kernel consisting of ideals of principal class in $k$. Thus $\mathfrak{A}_1 \sim \mathfrak{A}_2$ exactly when principal (integral) ideals $(B_1)$, $(B_2)$ exist in $K$ and (principal) ideals $\mathfrak{g}_1$, $\mathfrak{g}_2$ exist in $k$ for which

$$\mathfrak{A}_1(B_1)\,\mathfrak{g}_1 = \mathfrak{A}_2(B_2)\,\mathfrak{g}_2\,. \tag{10.2}$$

Thus $G'$ is a free group on $t$ generators subject to as many restrictions as there are independent relations

$$\mathfrak{R}_1^{g_1} \cdots \mathfrak{R}_t^{g_t} = \mathfrak{g}(B) \tag{10.3}$$

for $\mathfrak{g}$ an ideal in $k$ and $B$ an element of $K$. Some of these restrictions, (say $r_0$ of them), will be trivial, based on radicals $\alpha^{1/l} \in K$, where $\alpha \in k$, $\alpha^{1/l} \notin k$. Others (say $e$ of them) will be multiplicatively independent and nontrivial. Such (nontrivial) relationships are called *principal factorizations* of $K$ relative to $k$, or *principal factors* of the relative discriminant. Indeed, the order of $G$ is now

$$|\,G\,| = l^{t-e-r_0}\,. \tag{10.4}$$

While relative fields are now a traditional tool for even the cubic case [20, 16], our main interest is in principal factorization. We shall show (Theorem 15.7 below) that in some cases the existence of a principal factorization in the relative Kummer field enables us to deduce the existence of a principal factorization in the pure cubic field. In any case, it is illuminating to see a principal factorization of the pure cubic field "factored" into one of the relative Kummer field.[1]

## 11. Normal Field of Pure Cubic

We consider the pure cubic field as one of three conjugates

$$k_3 = Q(n^{1/3}), \qquad k_3' = Q(n^{1/3}\rho), \qquad k_3'' = Q(n^{1/3}\rho^2), \tag{11.1}$$

where $\rho = [-1 + (-3)^{1/2}]/2$ a cube root of unity. As before, the fundamental units are $\epsilon > 1$, $\epsilon'$, $\epsilon''$, $(\epsilon\epsilon'\epsilon'' = 1)$. The normal field is

$$k_6 = Q(n^{1/3}, \rho), \tag{11.2}$$

[1] In a later paper, one of the authors (Barrucand) will consider the problem of the normal field of a (general) cubic relative to the quadratic subfield.

and it shall, of course, be viewed as a field of relative degree 3 over

$$k_2 = Q(\rho). \tag{11.3}$$

The Galois group of $k_6$ is generated by two transformations, the cyclic operation $S$ given by

$$S(k_3, k_3', k_3'') = (k_3', k_3'', k_3) \tag{11.4a}$$

and the complex conjugation operation $T$ given by

$$T(k_3, k_3', k_3'') = (k_3, k_3'', k_3'). \tag{11.4b}$$

Thus $S\rho = \rho$ while $T\rho = \rho^2$, but $S(\rho n^{1/3}) = \rho^2 n^{1/3}$, and $T(\rho n^{1/3}) = \rho^2 n^{1/3}$. Also

$$S^3 = T^2 = I \qquad \text{and} \quad ST = TS^2. \tag{11.5}$$

We are interested in three relative norms of an element $F \in k_6$, namely,

$$N_2F = F \cdot TF \tag{11.6}$$

$$N_3F = F \cdot SF \cdot S^2F \tag{11.7}$$

$$N_6F = N_3(N_2F) = N_2(N_3F). \tag{11.8}$$

By the classical theory,

$$N_2F \in k_3, N_3F \in k_2, N_6F \in Q. \tag{11.9}$$

Similar relations hold, of course, for norms of ideals.

LEMMA 11.1. *If* $F \in k_6$, *then*

$$F^3 = F_3F_3^*F_3^{**}F_2, \tag{11.10}$$

*where*

$$F_3 \in k_3, \qquad F_3^* \in k_3', \qquad F_3^{**} \in k_3'', \qquad F_2 \in k_2. \tag{11.11}$$

*If* $F$ *is a unit, then so are the other factors shown here.*

*Proof.* $F^3 = (F \cdot TF)(F \cdot STF)(F \cdot S^2TF)/(TF \cdot STF \cdot S^2TF)$. Now

$$F \cdot TF = N_2F \in k_3.$$

Also, by (11.5),

$$F \cdot STF = S^2(SF \cdot TSF) = S^2N_2(SF) \in k_3'; \qquad \text{while} \quad F \cdot S^2TF \in k_3''.$$

Likewise,

$$TF \cdot STF \cdot S^2TF = N_3(TF) \in k_2 . \qquad \text{Q.E.D.}$$

## 12. Units in the Normal Field

If we let $U_6$, $U_3$, $U_3'$, $U_3''$, $U_2$ be the unit groups in $k_6$, $k_3$, $k_3'$, $k_3''$, $k_2$, respectively, we see that the product

$$U_0 = \{U_3 \times U_3' \times U_3'' \times U_2\} \tag{12.1}$$

is a subgroup of $U_6$ which may or may not be all of $U_6$. We shall call $u_6$ the *index* of this quotient

$$u_6 = | U_6/U_0 | . \tag{12.2}$$

Theorem 12.1. *There are two possibilities. Either*

$$u_6 = 1, U_6 = U_0 = \{\epsilon, \epsilon', -\rho\} \tag{12.3}$$

*(with $\epsilon$ a fundamental unit of $k_3$). Or,*

$$u_6 = 3, U_0 \subset U_6 = \{E_0 , SE_0 , -\rho\}, \tag{12.4a}$$

*where $E_0 \in U_6$, and for some fixed $c$ (mod 3),*

$$E_0^3 = \rho^c\epsilon/\epsilon'. \tag{12.4b}$$

*Proof.* From Lemma 11.1, if $E \in U_6$, $E^3 = \pm\rho^c\epsilon^a\epsilon'^b$. This leaves only a restricted number of choices of $a, b, c$ (mod 3). Note that $(\rho^c\epsilon)^{1/3} \notin k_6$, for the relation $X^3 = \rho^c\epsilon$ implies $(N_2X)^3 = \epsilon^2$ contradicting the fundamental property of the unit $\epsilon$. The choices are then reducible to (12.4b) or $E \in U_0$. The choice of $c$ is fixed (mod 3) since $\rho^{1/3} \notin k$. Q.E.D.

Lemma 12.2. *The relation* (12.4b) *is equivalent to*

$$\epsilon = \rho^d E_0/S^2E_0 = \rho^d E_1/SE_1 \tag{12.5}$$

*for $E_0$, $E_1 \in U_6$ and (using the exponent $c$ of* (12.4b)),

$$N_3(E_0) = \rho^c. \tag{12.6}$$

*Proof.* From (12.4b) $(SE_0)^3 = \rho^c\epsilon'/\epsilon''$, thus

$$(E_0/SE_0)^3 = \epsilon\epsilon''/(\epsilon')^2 = 1/(\epsilon')^3.$$

The $S^2$ operation gives (12.5). Conversely, starting with (12.5) for a unit $E_0 \in k_6$, we get

$$\epsilon/\epsilon' = E_0^3/N_3(E_0). \tag{12.7}$$

This identifies $\rho^c$ in (12.4b); also $E_1 = (S^2E_0)^{-1}$. Q.E.D.

LEMMA 12.3. *We have $u_6 = 3$ if and only if for some unit $E_1 \in k_6$ and exponent $d$* (mod 3) *we can write*

$$\begin{aligned} B_0 &= (n^{1/3})^d E_1 \\ \epsilon &= B_0/SB_0. \end{aligned} \tag{12.7a}$$

*We shall eventually see $d = 0$ always (by Corollary* 15.4.1).

## 13. USE OF HILBERT'S THEORY OF KUMMER FIELDS

We now consider ideal factorization in $k_6$. This can be done in straightforward fashion by combining the factorization rules (of Section 5) for $k_3$ with those of $k_2$ as follows:

If $p \equiv 1$ (mod 3) then $(p) = \pi\pi'$ in $k_2$, if $q \equiv 2$ (mod 3) $(q) = (q)$ in $k_2$; finally, $(3) = (1 - \rho)^2$.

We therefore obtain the following relative factorization rules:

(i) If $\pi \mid n$, $(\pi) = \mathfrak{P}^3$,

(ii) If $q \mid n$, $(q) = \mathfrak{Q}^3$,

(iii) If $\pi \nmid n$ and $(n/p)_3 = 1$, $(\pi) = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$,

(iv) If $\pi \nmid n$ and $(n/p)_3 \neq 1$, $(\pi) = (\pi)$,

(v) If $q \nmid n$ then $(q) = \mathfrak{Q}_1\mathfrak{Q}_2\mathfrak{Q}_3$,

(vi) If the field is of Dedekind type 1, $n \not\equiv \pm 1$ (9), then

$$(1 - \rho) = \mathfrak{T}^3 \qquad \text{(i.e., } S\mathfrak{T} = T\mathfrak{T} = \mathfrak{T}\text{)}$$

(vii) If the field is of Dedekind Type 2, $n \equiv \pm 1$ (9), then

$$(1 - \rho) = \mathfrak{T}_1\mathfrak{T}_2\mathfrak{T}_3, \qquad \text{(i.e., } T\mathfrak{T}_i = \mathfrak{T}_i \quad \text{but} \quad S\mathfrak{T}_i = \mathfrak{T}_{i+1}\text{)}.$$

By Hilbert's Theorem 148 [7], it is clear that the relative discriminant $\mathfrak{d}$ of $k_6/k_2$ is $k^2$, where $k = 3ab$ for Type 1 and $ab$ for Type 2. Thus the discriminant $\Delta_6$ of $k_6$ is related to the discriminant of $k_3$, $\Delta_3 (= 3k^2)$, by

$$\Delta_6 = 3\Delta_3^2. \tag{13.1}$$

In Hilbert's Theory an *ambiguous ideal* $\mathfrak{A}$ of $k_6/k_2$ is one for which $S\mathfrak{A} = \mathfrak{A}$ while $\mathfrak{A}$ is divisible by no ideal of $k_2$ except (1). An ambiguous ideal class $A$ of $k_6/k_2$ is one for which $SA = A$. Here ambiguity implies $A^3 = I$ but not conversely, of course.

Let $t_H$ be the number of totally ramified prime ideals in $k_6$. Then

$$t_H = t_3 + s_3\,, \tag{13.2}$$

where $t_3$ is the number of totally ramified primes in $k_3$ and $s_3$ is the number of those $\equiv 1 \pmod 3$. (Here $t_3$ and $s_3$ were called $t$ and $s$ in Section 2). Let $m_H = 1$ or 0 according as the solvability of a relative cubic analog of the Pell equation of norm $-1$, viz.,

$$N_3(E) = \rho \qquad E \in U_6\,. \tag{13.3}$$

Also let $n_H = 1$ or 0 according as the solvability of

$$N_3(X) = \rho \qquad X \in k_6 \tag{13.4}$$

(of course $X$ is not necessarily an integer so $m_H \leqslant n_H$). Then Hilbert's Theorems 158 and 159 yield the following:

THEOREM 13.1 (Hilbert). *The number of ambiguous ideal classes in $k_6/k_2$ generated by ambiguous ideals is $3^{v_H}$ where*

$$v_H = t_H + m_H - 2 \tag{13.5}$$

*The (unrestricted) number of ambiguous ideal classes in $k_6/k_2$ is $3^{u_H}$ where*

$$u_H = t_H + n_H - 2. \tag{13.6}$$

COROLLARY 13.1.1. *The number $e_H$ of (generating) principal factorizations of $k_6/k_2$ is given by*

$$e_H = 1 - m_H\,. \tag{13.7}$$

*The number of ambiguous classes without ambiguous ideals is given by*

$$f_H = n_H - m_H\,(\leqslant 1) \tag{13.8}$$

For proof, compare (13.5) and (10.4) with $t = t_H\,, e = e_H\,, r_0 = 1$. (Compare Theorem 3.1 to see the close analogy to the quadratic case.) Note that $e_H \geqslant e_3$ (the number of principal factorization in $k_3$).

LEMMA 13.2. *Equation* (13.3) *is solvable* ($m_H = 0, e_H = 1$) *only if all prime divisors of $n$ are $= 3$ or $\equiv \pm 1 \pmod 9$.*

*Remark.* The same condition is also necessary for $n_H = 1$, but we consider the special case for simplicity.

*Proof.* We express $E$ the solution of (13.3) in $k_6/k_2$ as $E = (A + B\rho)/C$ where $A, B, C \in k_3$. In general, $C \neq 1$, but note that the relative discriminant of $k_6/k_3$ has norm $\Delta_6/\Delta_3^2 = 3$ by (13.1). Therefore, $C$ can be chosen prime to any set of preassigned primes including all the divisors of $n$ (other than divisors of 3). If we expand $A, B, C$ in basis form as elements of $k_3$ we get (see (5.2)) for integers $\alpha, \beta, \gamma, \delta$ in $k_2$,

$$E = [\alpha + \beta(a^2b)^{1/3} + \gamma(ab^2)^{1/3}]/\delta, \tag{13.9}$$

where $n = a^2b$ in its usual representation, and $\delta$ is prime to all the divisors of $n$ (other than divisors of 3). The usual norm is now

$$N_3(E) = \frac{\alpha^3 + \beta^3a^2b + \gamma^3ab^2 - 3ab\alpha\beta\gamma}{\delta^3}. \tag{13.10}$$

Thus the solvability of (13.4) implies the solvability (in $k_2$) of

$$\xi^3 \equiv \rho \pmod{p} \tag{13.11}$$

for all $p(\neq 3)$ which divide $n$. It is an easy consequence of the "Euler criterion" that $p \equiv \pm 1 \pmod 9$ if (13.11) holds. Q.E.D.

## 14. Class Number Considerations

THEOREM 14.1. *Let $h_6$ be the class number of $k_6$ and let $h_3$ be the class number of $k_3$. Then*

$$h_6 = h_3^2(u_6/3). \tag{14.1}$$

COROLLARY 14.1.1. *If $3 \nmid h_3$ then $u_6 = 3$.*

Now Theorem 14.1 is classically known (see [20, 18]). Indeed, it is part of more general theories such as the Artin $L$-functions [17]. For our purposes, it may suffice to note an independent direct verification. Use the designation that $\zeta_t(s)$ is the Dedekind zeta-function of $k_t$, ($k_1 = Q$). Then

$$[\zeta_3(s)/\zeta_1(s)]^2\,[\zeta_2(s)/\zeta_1(s)] = [\zeta_6(s)/\zeta_1(s)] \tag{14.2a}$$

(as a direct consequence of the laws of factorization in Section 13). If we take the limit of each factor as $s \to 1$ we obtain [7, section 25],

$$[2\pi(\log \epsilon)\, h_3/\Delta_3^{1/2}]^2 \cdot [\pi/3^{3/2}] = [(2\pi)^3\, R_6h_6/(6\Delta_6^{1/2})], \tag{14.2b}$$

where $R_6$, the regulator of $k_6$, equals 3 $(\log \epsilon)^2/u_6$. From (13.1), we conclude (14.1).

The corollary is of great value in the classification problem in the next section. In the meantime, it might be remarked that Theorem 14.1 does not readily yield any new information on the class number $h_3$. If we use Theorem 13.1, with $u_6 = 3^{w_H}$

$$h_6 \geqq 3^{t_3+s_3+f_H-e_H-1}, \tag{14.3}$$

$$h_3^2 \geqq 3^{t_3+s_3+f_H-e_H-w_H}. \tag{14.4}$$

If we compare (14.4) with (2.3), we see the more easily calculated qualities agree, so (14.4) is no stronger (barring special information on the "difficult" quantities $e_H$, $w_H$, $f_H$, etc.).

## 15. Main Classification Theorem

We now give a broad classification of cubics according to properties visible in $k_6$. The classification, of course, includes the (previous) principal factorization in $k_3$ as one of many possibilities.

Lemma 15.1. *Let $A$ be an integer in $k_6$ such that the ideal $(A)$ is invariant under $S$,* i.e., $(A) = (SA)$. *Then $A$ can be factored uniquely into integers (except for units of $k_2$).*

$$A = \mu B. \tag{15.1}$$

*Here $\mu \in k_2$ and $B$ is made up wholly of totally ramified prime ideals of $k_6$ or their squares (cases* (i), (ii), (vi) *of Section* 13), *or else $B$ is a unit of $k_6$. ($A$ factor $(-\rho)^d$ is the trivial unit of $k_2$.)*

The proof is immediate from an examination of the cases. Here we use the fact that $k_2$ has class number unity (although it would suffice if it were prime to 3). Call such a $B$ and its ideal $(B)$ *primitive.*

Lemma 15.2. *The fundamental unit $\epsilon$ of $k_3$ satisfies*

$$\epsilon = B_0/SB_0 \tag{15.2}$$

*for a unique, primitive integer $B_0 \in k_3$ (except for unit factors such as $(-\rho)^d$).*

*Proof.* According to the usual procedure [7] of Hilbert's "Theorem 90", we can set

$$A_0 = 1 + \epsilon + \epsilon\epsilon'; \tag{15.3}$$

so $A_0 \neq 0$ (as $\epsilon' \notin k_3$). Trivially,

$$\epsilon = A_0/SA. \tag{15.4}$$

We can simplify $A_0$ according to Lemma 15.1 (since $S\mu = \mu$).

To see how $B_0$ is unique, set $\epsilon = B_0/SB_0 = B_1/SB_1$, and note $(B_0/B_1) = S(B_0/B_1) \in k_2$. Thus $B_0/B_1 = \mu/\mu_1$ and we are back to Lemma 15.1. Q.E.D.

By direct computation, the $N_2A_0$ operation gives

$$N_2A_0 = (1 + \epsilon + \epsilon\epsilon')(1 + \epsilon + \epsilon\epsilon'') = \epsilon(\xi + \xi' + \xi''),$$

where $\xi = 1 + \epsilon + 1/\epsilon$, (using only $\epsilon\epsilon'\epsilon'' = 1$). This leads to the following result:

LEMMA 15.3. *If* $\mathrm{Tr}(\xi) = (\xi + \xi' + \xi'')$ *for* $\xi \in k_3$, *then*

$$N_6(1 + \epsilon + \epsilon\epsilon') = [3 + \mathrm{Tr}(\epsilon) + \mathrm{Tr}(1/\epsilon)]^3. \tag{15.5}$$

THEOREM 15.4. *The primitive ideal* $(B_0)$ *for which* $\epsilon = B_0/SB_0$, *satisfies either*

$$(B_0) = (1), \quad \text{and} \quad u_6 = 3, \tag{15.6a}$$

*or*

$$(B_0) = \mathfrak{P}\mathfrak{P}^2 \cdots, \quad \text{and} \quad u_6 = 1, \tag{15.6b}$$

*where* $\mathfrak{P} \mid \pi \mid p \mid n$ $[p \equiv 1 \pmod 3]$ *and* (15.6b) *is a product of some possible (triple) factors of the type shown.*

For proof, start with the decomposition $A_0 = \mu B_0$ where $N_6A_0$ and $N_6\mu$ are perfect cubes by Lemma 15.3. Hence if $B_0$ is not a unit it must be of the type shown (recall $\mathfrak{P}^3 = (\pi) \in k_2$). Now by Lemma 12.3, $u_6 = 3$ corresponds to $(B_0) = (n^{d/3})$ for some $d$. Since this form of $(B_0)$ agrees with neither type (15.6a) nor type (15.6b), unless $d \equiv 0 \pmod 3$, it is clear that we have also proved the following result:

COROLLARY 15.4.1. *The value of d in Lemmas* 12.2 *and* 12.3 *is always* $= 0$.

Now when $(B_0) = (1)$, choose the sign $\pm B_0$ so that $N_3(B_0) = \rho^c$. Then the distinction arises based on whether or not $N_3(B_0) = 1$ (or $\rho^c \neq 1$). If $N_3(B_0) = 1$, a further application of Hilbert's Theorem 90 yields

$$B_0 = B_1/SB_1\,, \tag{15.7}$$

where $B_1$ can (usually) be found by such classic devices as the primitive part of $A_1 = B_1\mu_1$, where

$$A_1 = 1 + B_0 + B_0 \cdot SB_0 \tag{15.8}$$

(assuming $A_1 \neq 0$). On this basis, it is no longer possible for $B_1$ to be a unit, because the relation

$$\epsilon = B_0/SB_0 \tag{15.9}$$

makes $[B_0\,, SB_0]$ a system of units of index 3 (see Theorem 12.1). A new system $[B_0\,, SB_1]$ would give $u_6 = 9$, which is excluded.

Thus with $B_0$ a unit of norm 1, a further classification is based on the study of the nonunit $B_1$ whose ideal $(B_1)[= (SB_1)$ from (15.7)] is composed entirely of the ramified prime ideals in $k_6/k_2$. Since there can be only one principal factorization generated by Corollary 13.1.1, $B_1$ and $TB_1$ (the complex conjugate (must generate the same set. Thus either

$$(B_1) \sim (TB_1), \tag{15.10}$$

or

$$(B_1)(TB_1) \sim 1. \tag{15.11}$$

(The symbol $(A) \sim (B)$ means that the ideals differ by cubed factors or factors of $n^{1/3}$.)

LEMMA 15.5. *The alternative* (15.11) *or* (15.6b) *is possible only when n has a prime divisor* $\equiv 1 \pmod 3$.

The proof is seen by examining possible factorizations, as in Theorem 15.4. It is clear from (15.11) that $B_1$ also has the form (15.6b). (More importantly, we shall note in Section 16 that (15.6b) does occur for some $n$ (e.g., $n = 7$) *but* (15.11) *is conjectured to never occur.*) In the case (15.10) we see that $(B_1)^2 = (B_1 \cdot TB_1)$ is generated by an *element of* $k_3$, which must be a principal factor of $k_3$ in our usual sense!

THEOREM 15.6. *The fields are of the following four types based on the quantities* $B_0$ *and* $B_1$ *given by*

$$\epsilon = B_0/SB_0 \qquad (N_3B_0 = \rho^c), \tag{15.12}$$

$$B_0 = B_1/SB_1 \qquad (\textit{when } N_3B_0 = 1): \tag{15.13}$$

*Type I.* *Principal factorization in $k_3$ (and $k_6$ hence unit-index 3):*
$(B_0) = (1), N_3B_0 = 1, e_3 = 1, e_H = 1, u_6 = 3.$

*Type II.* *Principal factorization in $k_6$ (only) with unit-index 3:*
$(B_0) = (1), N_3B_0 = 1, e_3 = 0, e_H = 1, u_6 = 3.$

*Type III.* *Principal factorization in $k_6$ (only) with unit-index 1:*
$(B_0) = \mathfrak{P}\bar{\mathfrak{P}}^2 \cdots, N_3B_0 = \pi^3, \ldots, e_3 = 0, e_H = 1, u_6 = 1.$

*Type IV.* *Principal factorization does not occur, so unit has norm $\rho$:*
$(B_0) = (1), N_3B_0 = \rho^c (\neq 1), e_3 = 0, e_H = 0, u_6 = 3.$

The proof consists of a survey of the cases. In Type I, $(B_1 \cdot TB_1) \in k_3$ represents the principal factorization in $k_3$ corresponding to $B_1$ in $k_6$. In Type II, $(B_1) = \mathfrak{P}\bar{\mathfrak{P}}^2 \cdots$; while in Type III, $(B_0) = \mathfrak{P}\bar{\mathfrak{P}}^2 \cdots$, leading to a principal factorization in $k_6$ which does *not* project into $k_3$.

Now if we combine Lemma 15.5, used to exclude Types II and III, with Lemma 13.2, used to exclude Type IV, we have a condition which implies Type I. (This is something we were unable to achieve in [15] by purely rational methods).

THEOREM 15.7. *Let $n$ have no factors $p \equiv 1$ (mod 3) and let $n$ have at least one factor $\equiv 2$ or 5* (mod 9). *Then there exists a principal factorization in $Q(n^{1/3}) = k_3$.*

## 16. DIOPHANTINE NORM EQUATIONS

Theorem 15.7 may be put in the form of diophantine norm equations. For example, if $q$ is a prime $\equiv 2$ or 5 (mod 9) we can set $n = 3^t q$, $(t = 0, 1, 2)$, and the existence of principal factorization implies (by Section 7) that the equations $N(\alpha) = 3$ and $q$ are solvable for $\alpha \in k_3$. Thus if we expand $\alpha$ into its basis we see the norm equations in $(x, y, z)$

$$(n = 3^t q)\, x^3 + 3^t q y^3 + 3^u q^2 z^3 - 3^{(t+u+3)/3} qxyz = 3 \text{ and } q \quad (16.1)$$

are solvable for $(t, u) = (0, 0), (1, 2)$, and $(2, 1)$.

We can take $n = 3^t q_1 q_2$ or $3^t q_1 q_2^2$ where both $q_i \equiv -1$ (mod 3), $n \not\equiv \pm 1$ (mod 9) and at least one $q_i \equiv 2$ or 5 (mod 9); then the cases become more highly proliferated. The best "general" result we can get is each of these diophantine equations:

$$(n = 3^t q_1 q_2)\, x^3 + 3^t q_1 q_2 y^3 + 3^u q_1^2 q_2^2 z^3 - 3^{(t+u+3)/3} q_1 q_2 xyz = m, \quad (16.2a)$$

$$(n = 3^t q_1 q_2^2)\, x^3 + 3^t q_1 q_2^2 y^3 + 3^u q_1^2 q\, z^3 - 3^{(t+u+3)/3} q_1 q_2 xyz = m, \quad (16.2b)$$

are solvable for $(t, u) = (0, 0)$, $(1, 2)$, and $(2, 1)$, where $m$ *is either* 3, $q_1$, $q_2$ *or a product of two of these factors.*

Of course when $t = u = 0$ and $n \equiv \pm 1 \pmod 9$, then our field is of "Type 2", and 3 is not totally ramified (see Section 5). Here $N(\alpha) = q_i$ would easily be solvable but the representation of $\alpha$ might require the full basis. This leads to the representation of $m = 27q_1$ and $27q_2$, by (16.2a) or (16.2b) (whichever applies). (Compare [22].)

## 17. Numerical Data

Let us apply the above classification to $Q(n^{1/3})$ for cube-free $2 \leqslant n < 50$, using Selmer's table [14] for comparison.

*Type I. Principal factorization in* $k_3$

$n = 2, 5, 6, 10, 11, 12, 14, 15, 18, 20, 22, 23, 29, 30, 33, 34, 38, 41, 42, 44, 45, 46, 47.$

In these cases, for some $\alpha \in k_3$, $\epsilon = \alpha^3/N_3\alpha$. Thus in (12.4b), $c = 1$ and the nonprimitive unit has the value

$$E_0 = \alpha/\alpha'. \tag{17.1}$$

Principal factorizations of $\alpha$ are given in Selmer's table for all these cases. Actually, Theorem 15.7 accounts for all cases except 14, 38, 42, where a prime divisor is $\equiv 1 \pmod 3$.

*Type II. Principal factorization in* $k_6$ *(only) with unit-index* 3

(No cases seem to occur.)

*Type III. Principal factorization in* $k_6$ *(only) with unit-index* 1

This is the case where the units of $k_6$ are generated only by the subfields. In each case, we must show the impossibility of $(\epsilon\rho^c/\epsilon')^{1/3} \in k_6$. It can be done most conveniently by finding a prime $P$ such that

$$(n/P)_3 = 1, \qquad P \equiv 1 \pmod{18}. \tag{17.2}$$

For such a $P$ the factorization $(P) = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$ is valid and $N_6\mathfrak{P}_i = N_6\mathfrak{P}_i = P$. Thus every integer in $k_6$ is congruent to a rational integer (mod $\mathfrak{P}_i$) and $\rho \equiv m^3 \pmod P$. Thus it suffices to show that $\epsilon, \epsilon', \epsilon''$ are congruentially equivalent to numbers of *different* cubic residue character. Suitable values of $P$ for each $n$ are as follows:

| $n$ | 7 | 13 | 19 | 21 | 26 | 28 | 31 | 35 | 37 | 39 | 43 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $P$ | 19 | 163 | 109 | 73 | 19 | 163 | 19 | 271 | 19 | 19 | 37. |

As an illustration of (15.6b), when $n = 7$,

$$B_0 = 7^{1/3}(7^{2/3} + \rho 7^{1/3} - (3 + 2\rho))/(-3)^{1/2};$$

so $(B_0) = \mathfrak{P}^2\bar{\mathfrak{P}}$ if $\mathfrak{P}^3 = (3 + 2\rho)$, $\bar{\mathfrak{P}}^3 = (3 - 2\rho)$.

*Type IV. Principal factorization does not occur; so unit has norm* $\rho$

Here a unit $E_0 \in k_6$ has $N_3 E_0 = \rho^c (\neq 1)$. Only these two cases occur where $t_3 = 1$, $3 \nmid h_3$ (hence $e_3 = 0$, while $u_6 = 3$ by Corollary 14.1.1):

$$n = 3, \qquad E_0 = [1 - \rho^2(-3)^{1/2} - 3^{2/3}/(-3)^{1/2}]$$

$$n = 17, \qquad E_0 = [7(2 + (-3)^{1/2}) + (2 - (-3)^{1/2})^2\, 17^{1/3} + (2 + (-3)^{1/2})\, 17^{2/3}\rho]/(-3)^{1/2}.$$

Actually the range described here ($n \leqslant 50$) is barely the beginning of the study of interesting cases. Some unpublished calculations of Barrucand, for example, are listed for principal factors

$$\alpha = A + B\theta + C\theta^2, \qquad \theta = n^{1/3}, \tag{17.3}$$

together with the values of Selmer for the class number $h_3$ [14, 21] and the number $f_3$ of independent "special ambiguous classes" (called $f$ in Section 2):

| $n$ | $A$ | $B$ | $C$ | $\lvert N(\alpha)\rvert$ | $h_3$ | $f_3$ |
|---|---|---|---|---|---|---|
| 51 | 330 | 89 | 24 | 3 | 3 | 1 |
| 61 | 16 | 4 | 1 | 9 | 6 | 1 |
| 67 | 16 | 4 | 1 | 9 | 6 | 1 |
| 103 | 912675 | 194702 | 41536 | 3 | 3 | 1 |
| 151 | 38905 | 7306 | 1372 | 9 | 6 | 1 |

All these cases are of Type I (see (4.7) above). The first ($n = 51$) is a special type omitted from Corollary 4.2.1. The other values of $n$ are primes $p$, ($4p = x^2 + 243y^2$), where $(3/p)_3 = 1$.

## ACKNOWLEDGMENTS

The authors are indebted to Dr. H. Hasse for making available his unpublished work [17] on relative class structure, and to Dr. E. S. Selmer for making available the unpublished supplement [21] to his tables [14].

*Note added in proof.* A recent paper of Honda [23] sharpens Corollary 4.2.1 (see [15]) to a necessary and sufficient condition and shows $h_3 \not\equiv 0 \pmod 3$ for $n = p \equiv -1 \pmod 3$. (See Abstract and Section 17, Type IV above.)

## REFERENCES

15. P. BARRUCAND AND H. COHN, A rational genus, class number divisibility, and unit theory for pure cubic fields, *J. Number Theory* **2** (1970), 7–21.
16. J. W. S. CASSELS, The rational solutions of the diophantine equation $Y^2 = X^3 - D$, *Acta Math.* **82** (1950), 243–273.
17. H. HASSE, Artinsche Führer, Artinsche $L$-Funktionen und Gaussche Summen über endlich-algebraischen Zahlkörpern, *Acta Salmanticensia* **4** (1954), 1–113.
18. H. HASSE, The class number formula of Dedekind-Meyer for simply real cubic number fields, unpublished manuscript.
19. H. B. MANN, "Introduction to Algebraic Number Theory," Ohio State Univ. Press, Columbus, Ohio, 1955.
20. C. MEYER, "Die Berechnung der Klassenzahl Abelscher Zahlkörper über quadratischen Zahlkörpern," Akademie Verlag, Berlin, 1957.
21. E. S. SELMER, Supplement to tables for the purely cubic field $K(m^{1/3})$, unpublished manuscript.
22. E. S. SELMER, Sufficient existence conditions for the existence of rational points on certain cubic surfaces, *Math. Scand.* **1** (1953), 113–119.
23. T. HONDA, Pure cubic fields whose class numbers are multiples of three, *J. Number Theory* **3** (1971), 7–12.